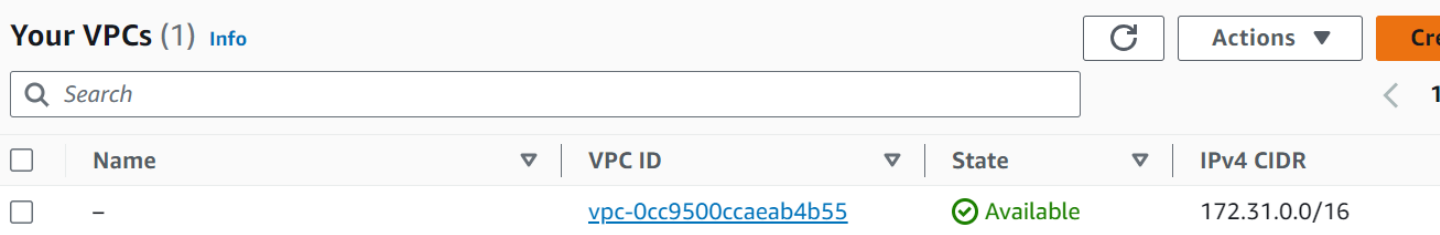
AWS DOCUMENTATION (VPC-peering connections with different region)

Creating the VPC and Subnets in the Singapore Region

1)CREATE THE VPC IN SINGAPORE REGION

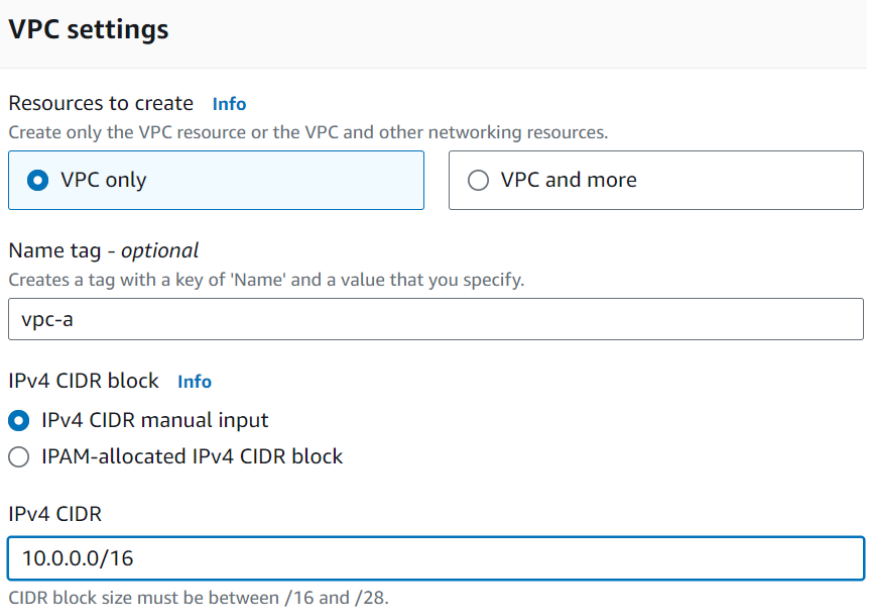
Step I : Select the region and go to VPC service.

Step II : Click on create VPC.

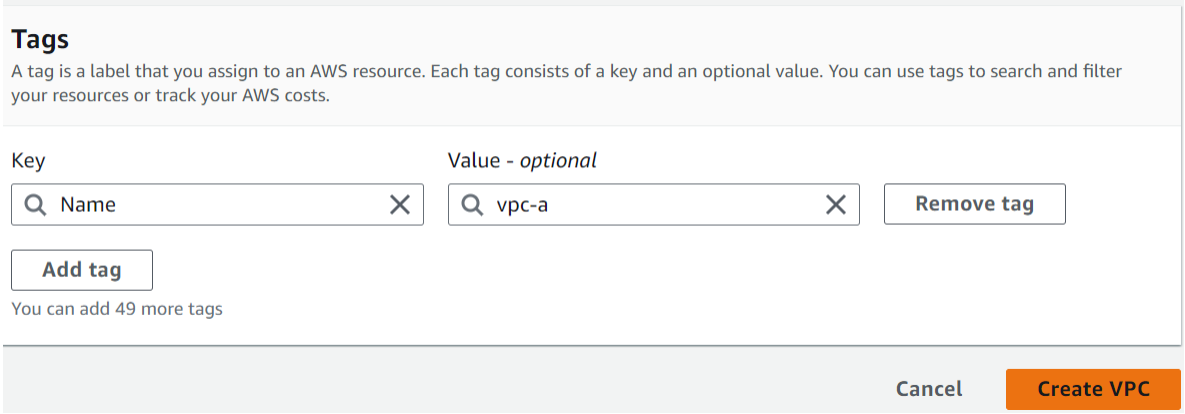


Step III : Select VPC only.

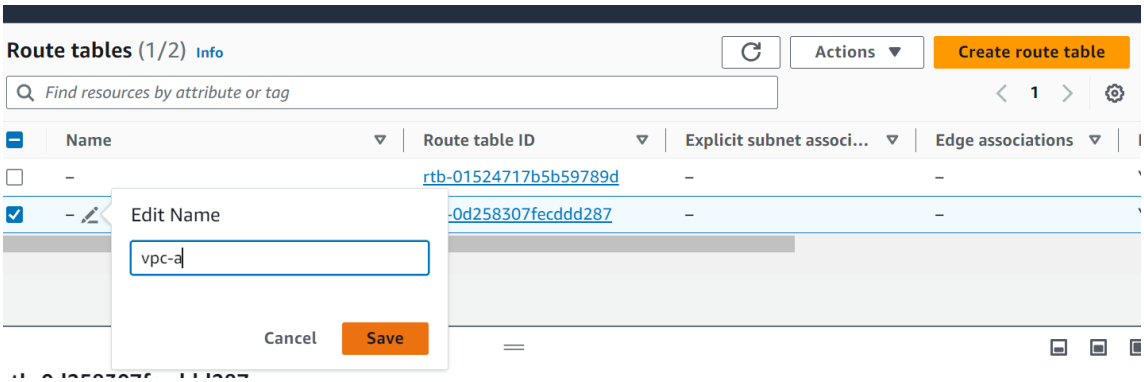
Step IV : Provide name and IPV4 CIDR for the VPC.



Step V : Click the Create VPC.

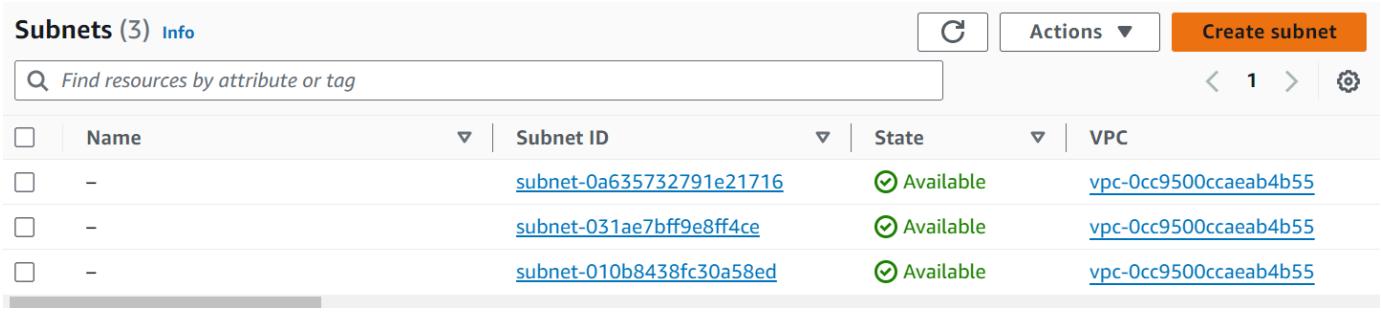


Automatically route table is created give it name.



2) CREATE SUBNETS

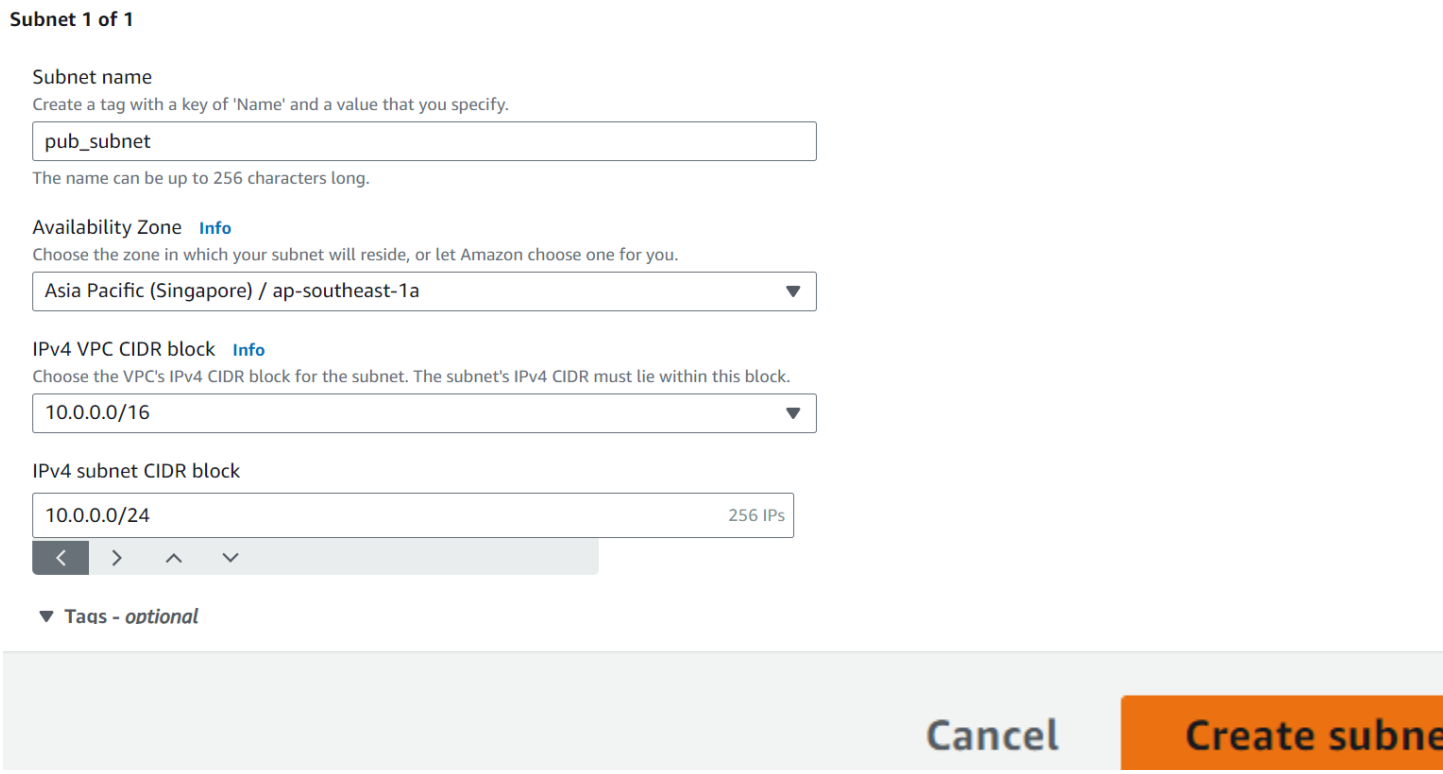
Step I : click on Subnets and then create Subnet.



Step II : Select the newly created subnet.

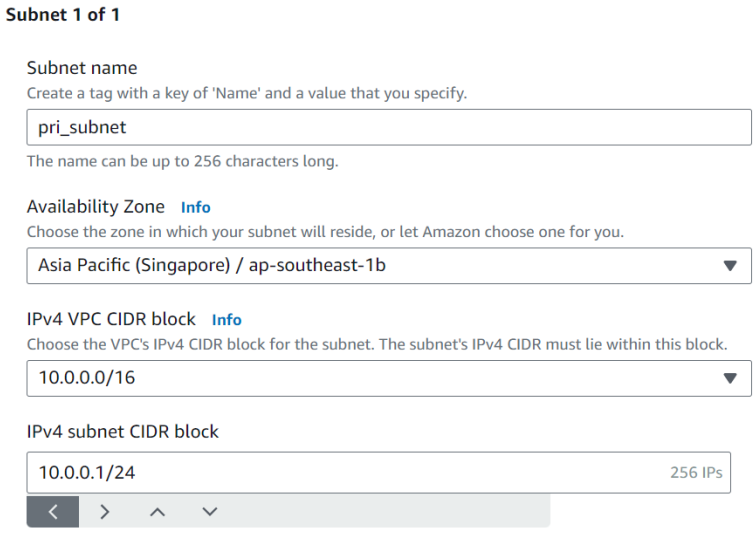
Step III : Create a public subnet:

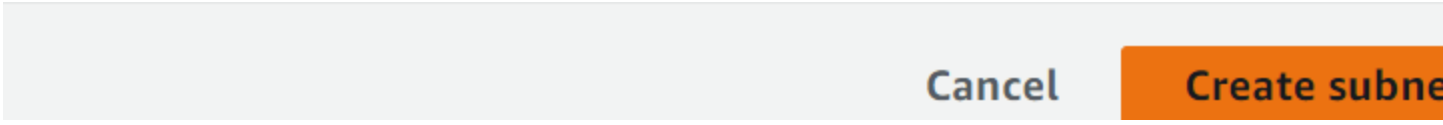
Enter subnet Details(name, availability zone,IPv4 CIDR block)



Step IV : Create private subnet:

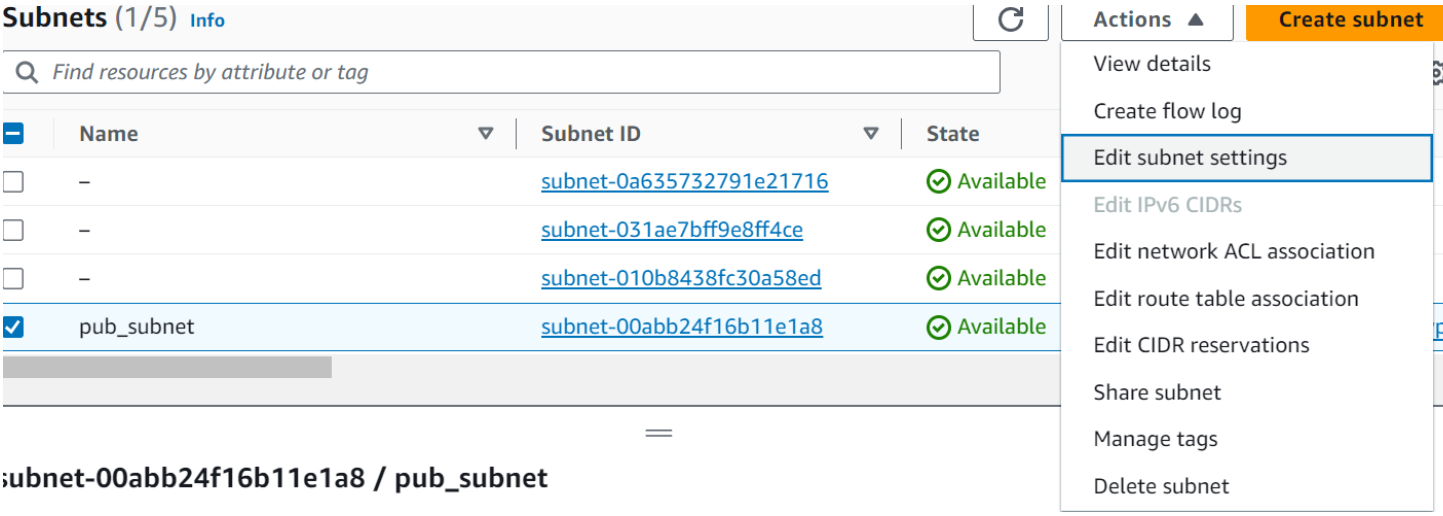
Repeat same process for private subnet.

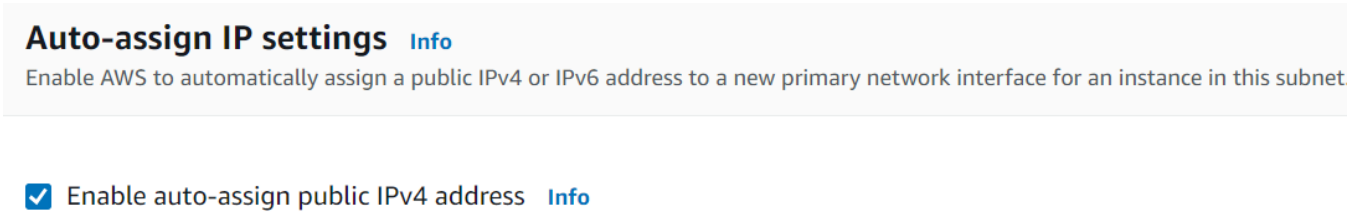




3)CONFIGURE SUBNET SETTINGS

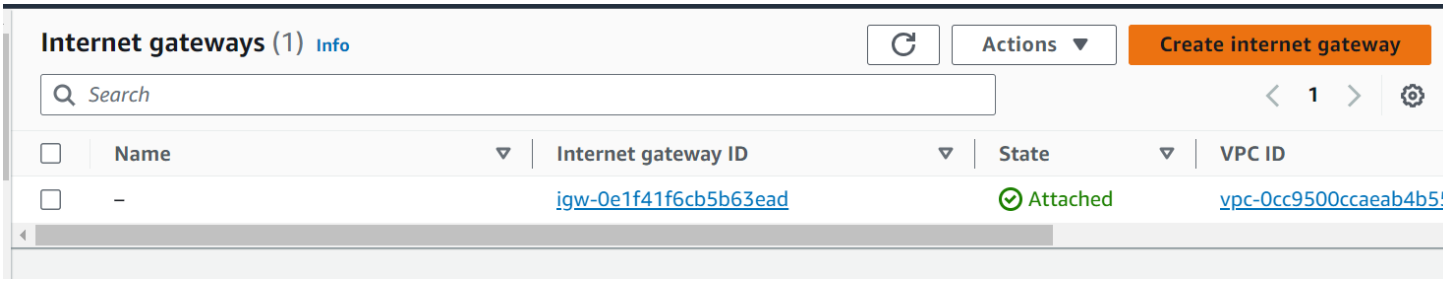
Step I : Enable the auto- assign public IPv4 address for the public subnet.

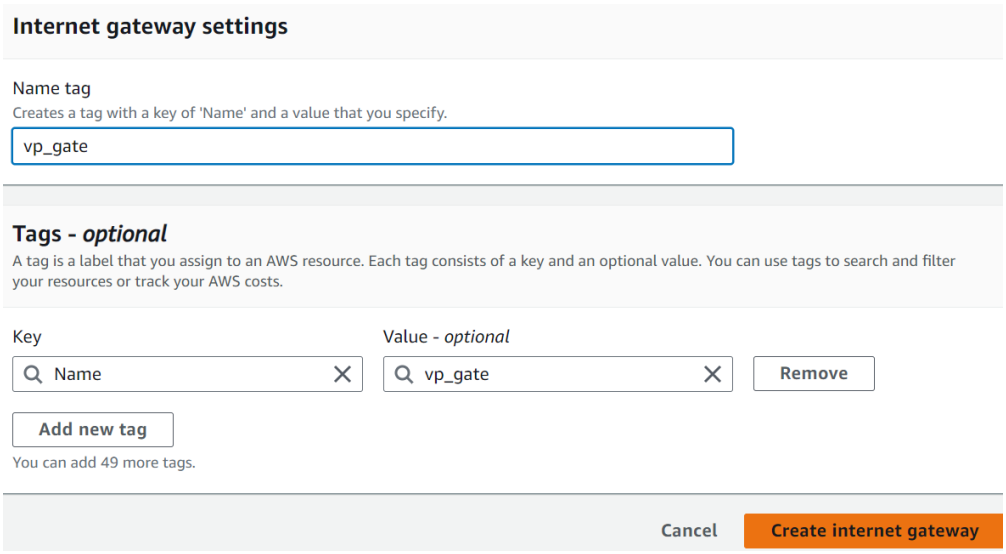




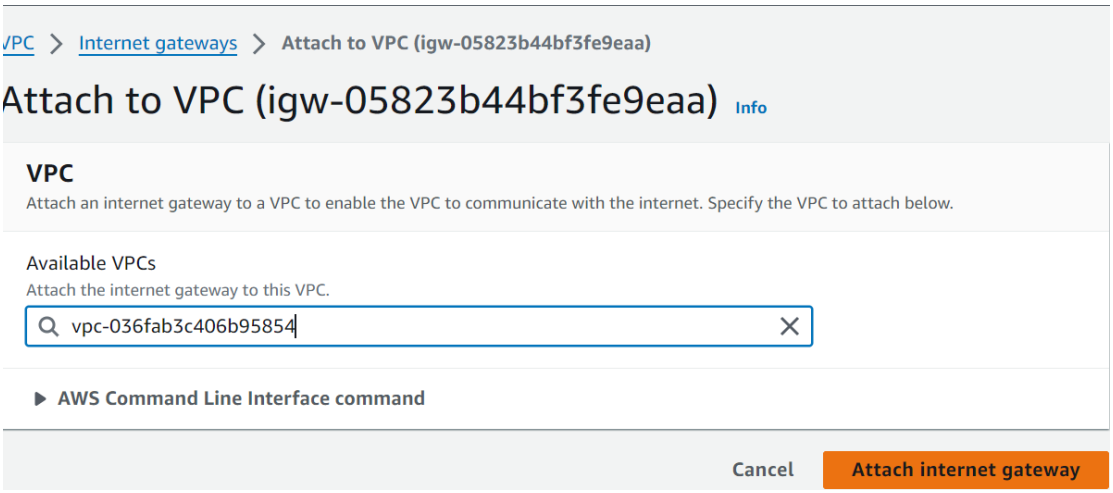
4)CREATE AND ATTACH GATEWAY

Step I : Create the Internet Gateway.



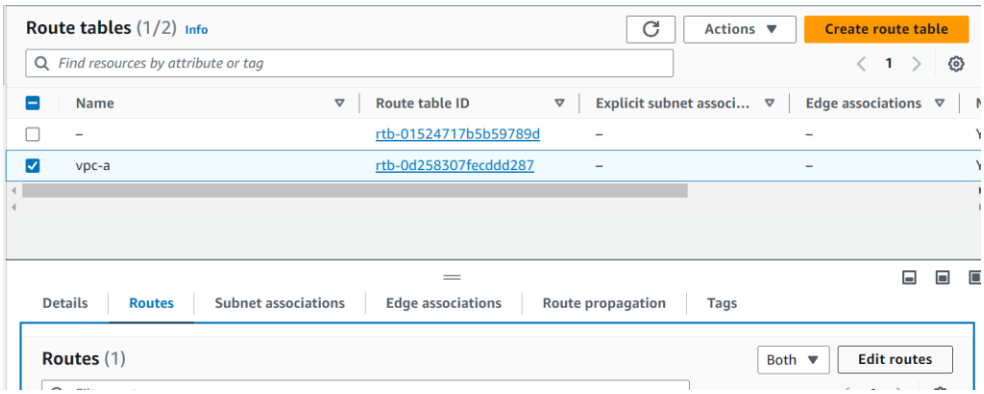


Step II : Attach the internet Gateway to the VPC.



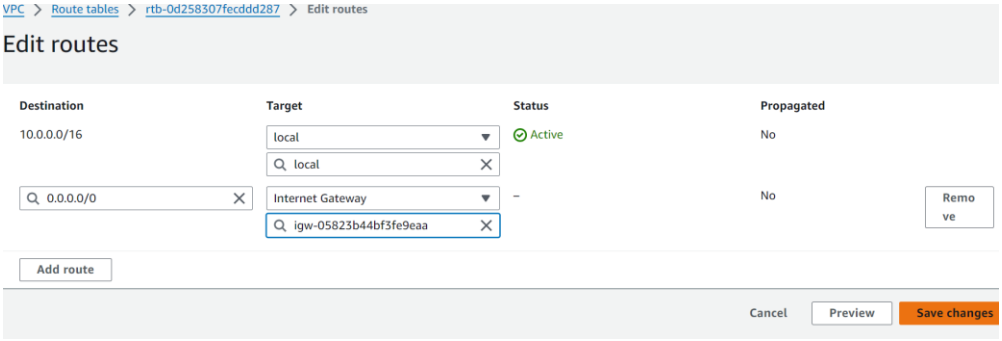
5)UPDATE ROUTE TABLE

Step I : Go to Route Tables.



Step II : Edit routes to add an internet gateway route.

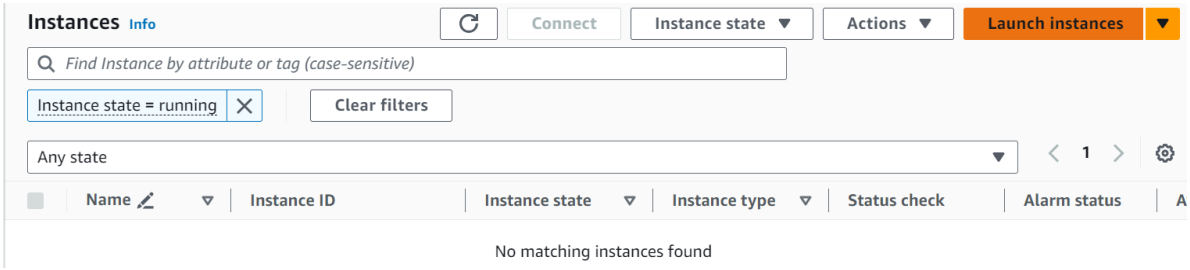
Step III : then Save Changes.



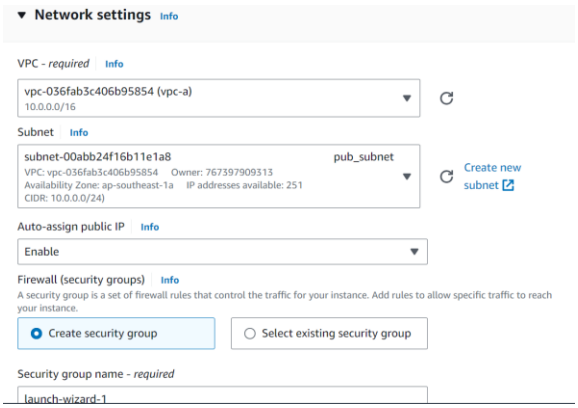
Launch Instances in Singapore region

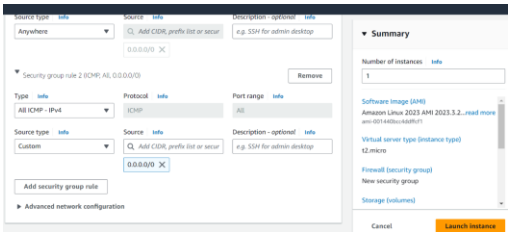
1)LAUNCH PUBLIC INSTANCE

Step I : Go to EC2 service,Launch the instances in public subnet.



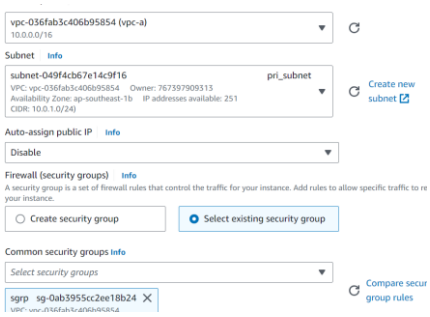
Step II : choose the key-pair,network settings and launch the instance.





2)LAUNCH PRIVATE INSTANCE

Step I : Launch another Instance in the Private subnet.

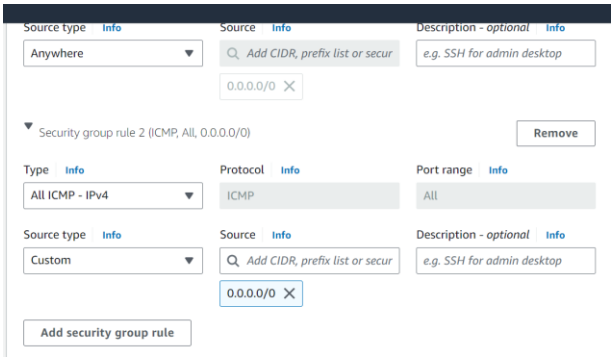


Step II : follows similar steps as for the public instance.

3) CONFIGURE SECURITY GROUP RULES

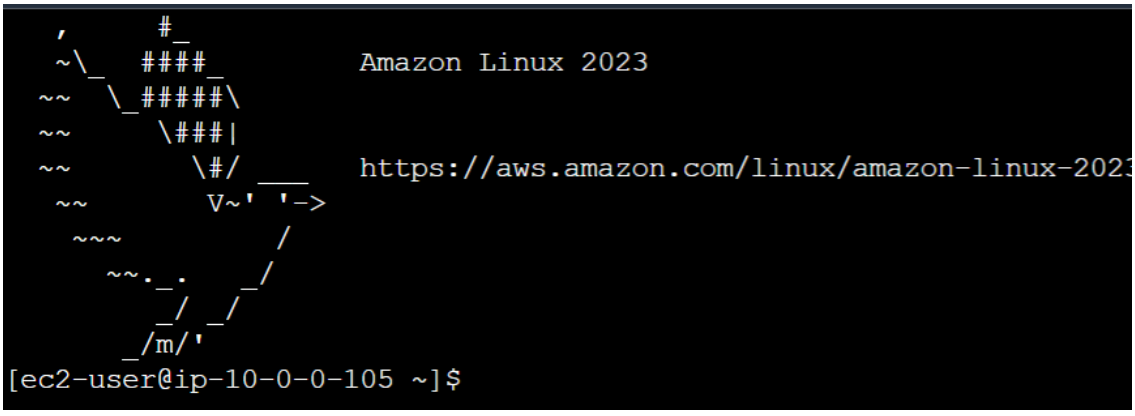
Step I : Edit Inbound rules for both the instances in Security group.

Step II : Add all ICMP in anywhere in both security groups.



4)CONNECT THE INSTANCES

Step I : Connect to the public Instance.



Ping the private instance .

```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-0-105 ~]$ ping 10.0.1.84
PING 10.0.1.84 (10.0.1.84) 56(84) bytes of data.
64 bytes from 10.0.1.84: icmp_seq=1 ttl=127 time=1.50 ms
64 bytes from 10.0.1.84: icmp_seq=2 ttl=127 time=1.12 ms
64 bytes from 10.0.1.84: icmp_seq=3 ttl=127 time=1.09 ms
```

Step II : Copy the private key of private instances and paste it in vim shree.pem and give the rw permission.

Step III : to give remote access of private instance give command ssh -i “keyname” ec2-user@privateIP.

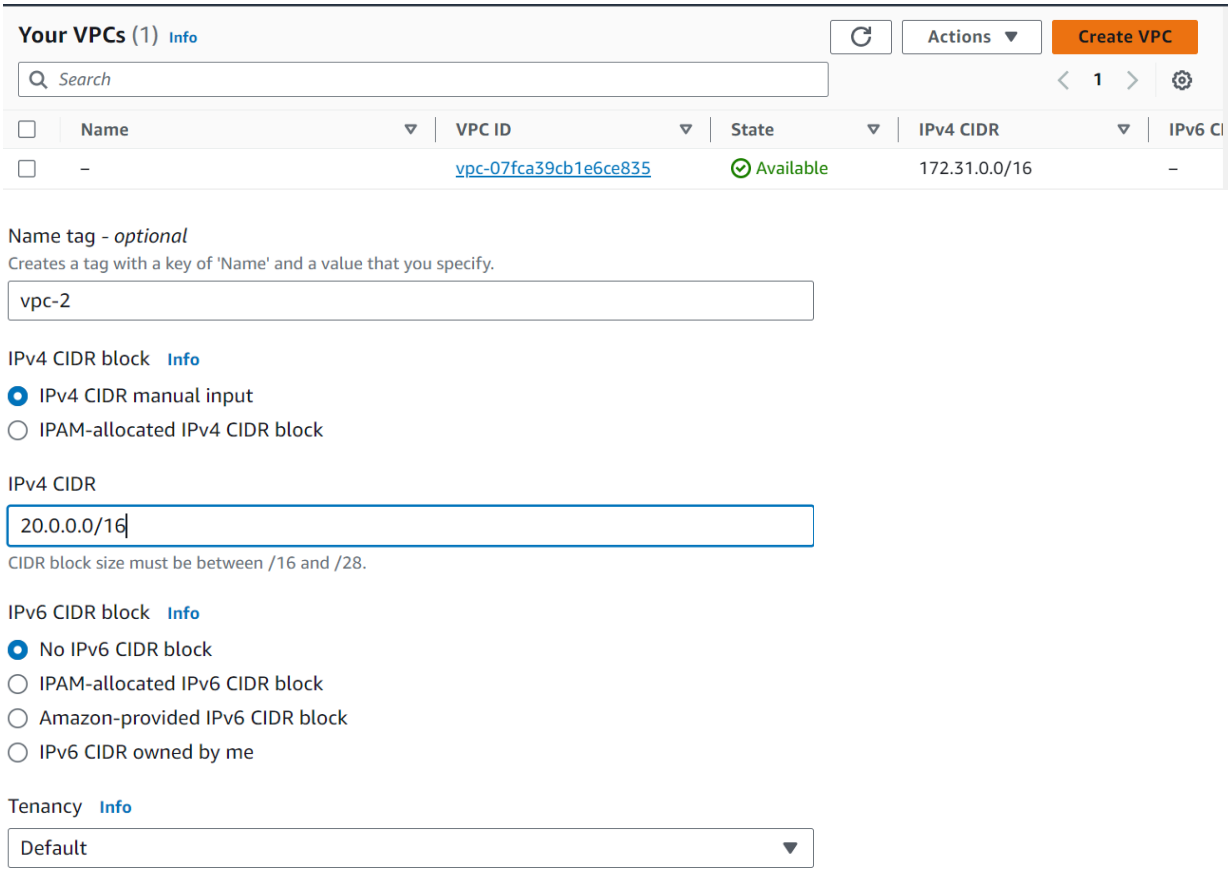
Step IV : here ,we can remotely access the private IP.

```
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 1.052/1.816/6.471/1.764 ms
[ec2-user@ip-10-0-0-105 ~]$ vim shree.pem
[ec2-user@ip-10-0-0-105 ~]$ chmod 600 shree.pem
[ec2-user@ip-10-0-0-105 ~]$ ssh -i shree.pem ec2-user@10.0.1.84
The authenticity of host '10.0.1.84 (10.0.1.84)' can't be established.
ED25519 key fingerprint is SHA256:92M2WR8ixF25wgaaHUAl/LY+HF3t63d5K5cVmCk/wd0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.84' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-1-84 ~]$
```

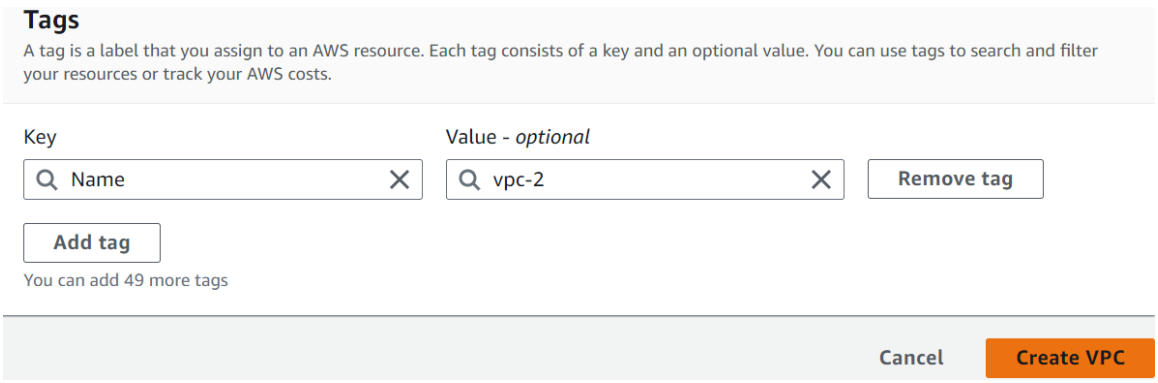
Creating the VPC and Subnet in Paris region

1)CREATE THE VPC IN PARIS REGION

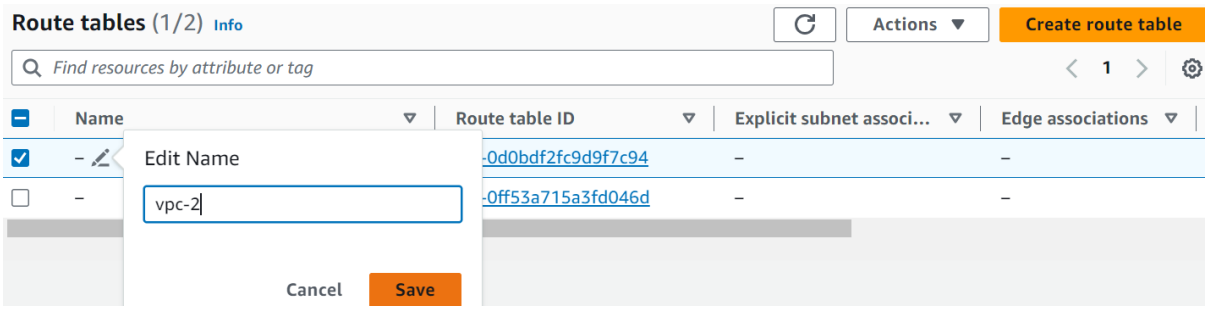
Step I : In paris region ,go to VPC service.



Step II : click on create VPC with the name and IPv4 CIDR and click om create.

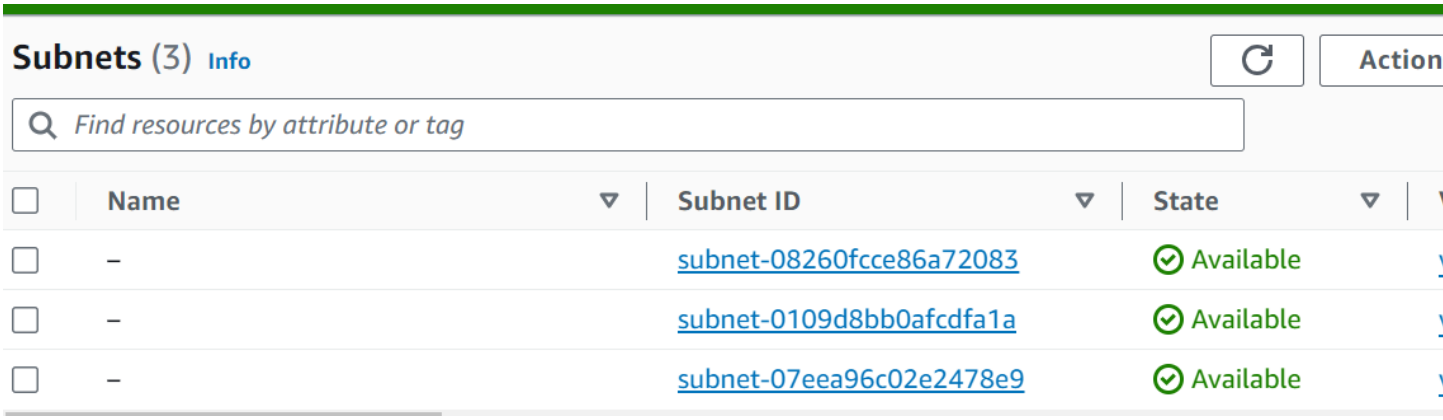


Step III : Automatically,route table is created give its name.

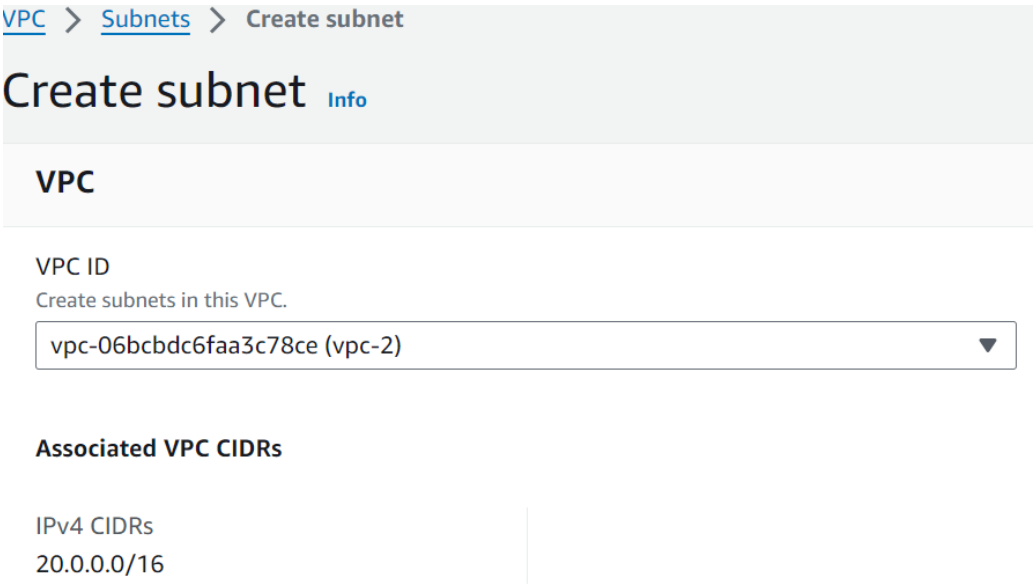


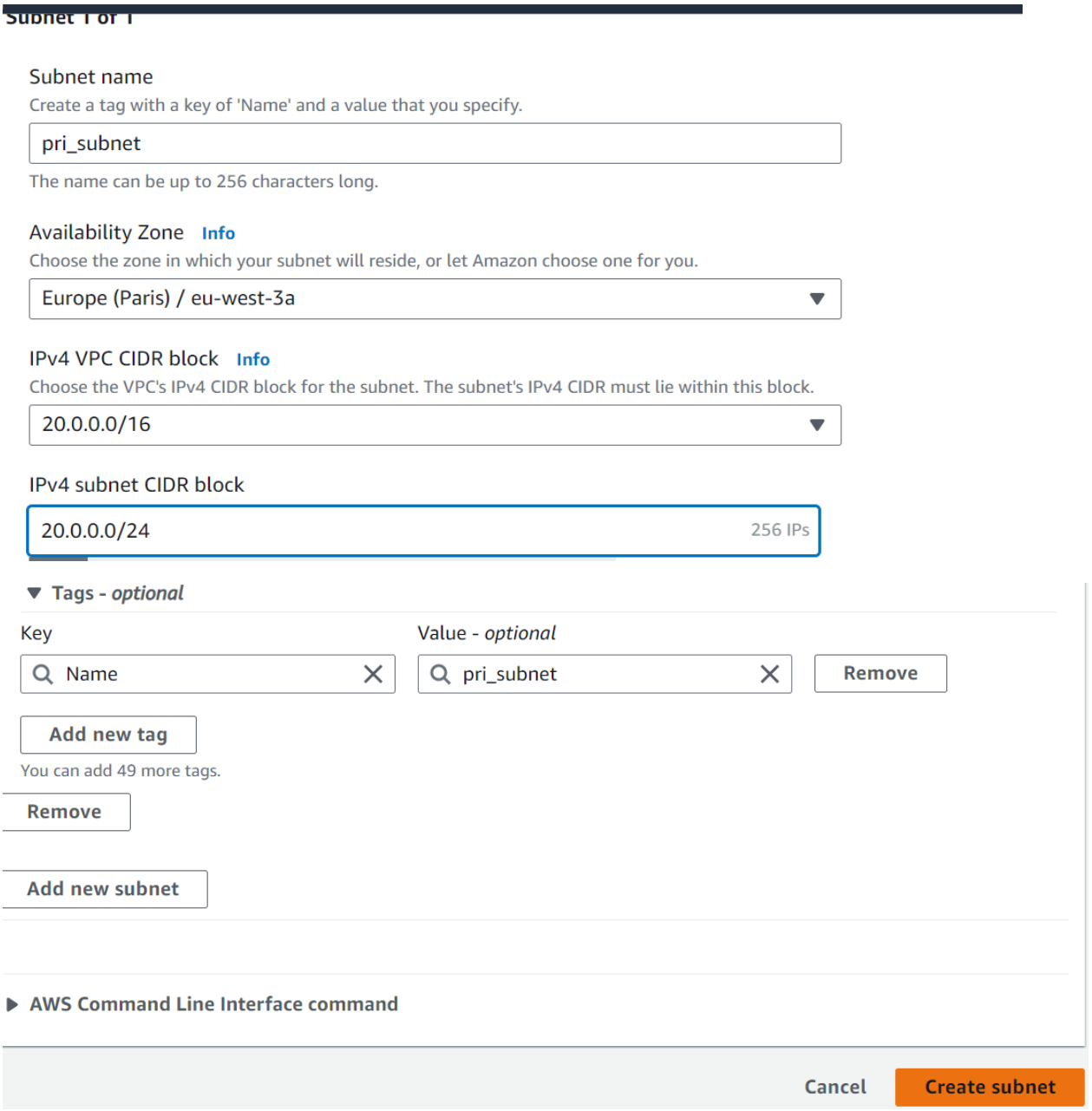
2)CREATE SUBNET IN PARIS REGION

Step I : Go to Subnets, click on create Subnets.



Step II : Create the private subnet in Paris region follows the step as in Singapure region.



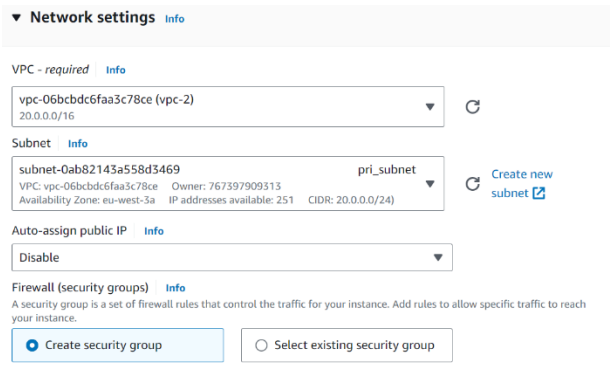


Launch Instance in Paris region

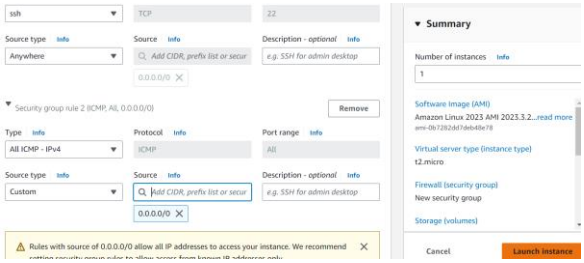
3)LAUNCH PRIVATE INSTANCE IN PARIS REGION

Step I :Go to in EC2 Service, click on launch Instance.

Step II : Give the name to instance and all needed things.



Step III : In Security group, add inbound rule All ICMP .



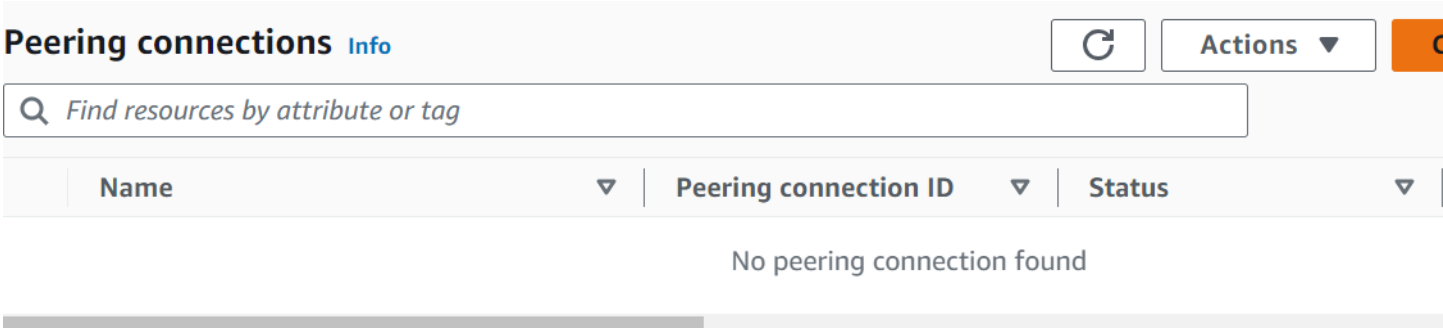
Step IV : Launch it.

Set up the VPC Peering

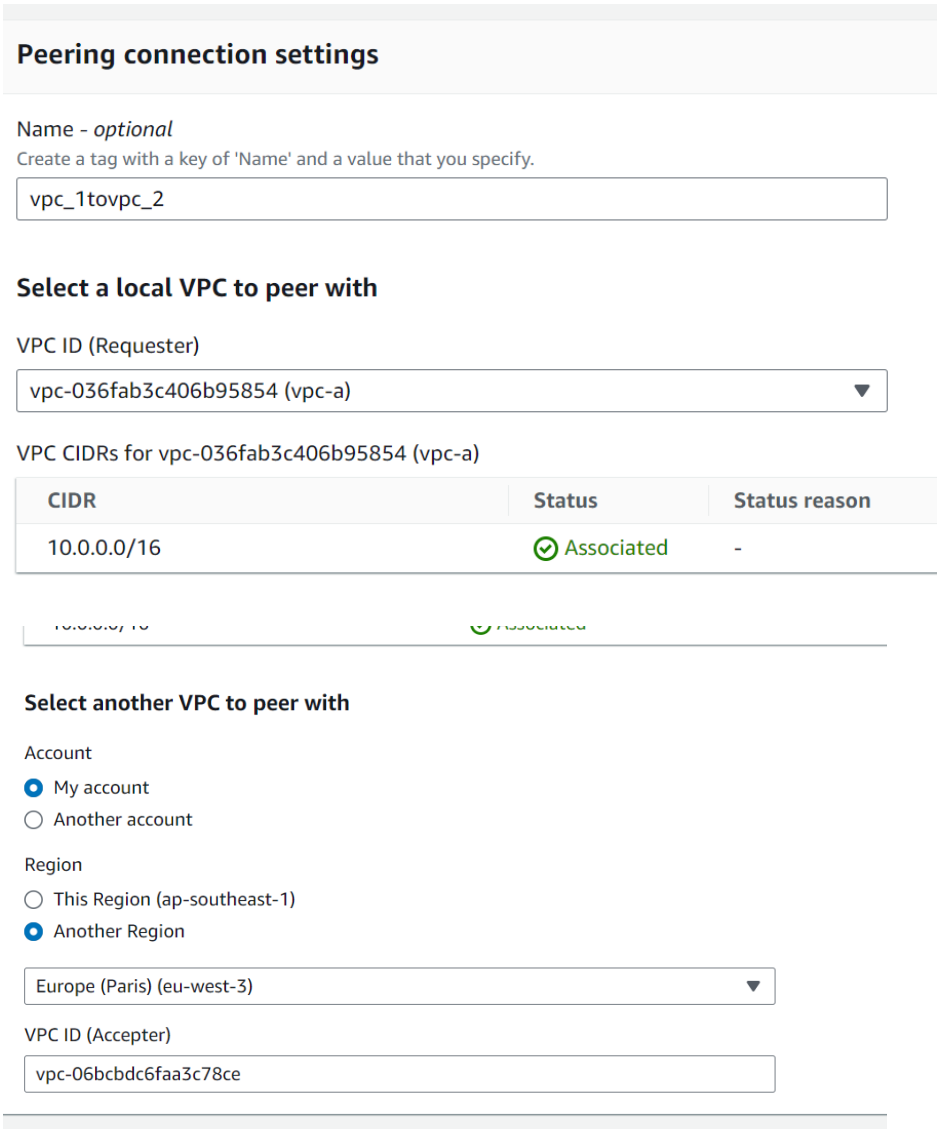
1)CREATE PEERING CONNECTION

Step I : Go to Singapore region and click VPC.

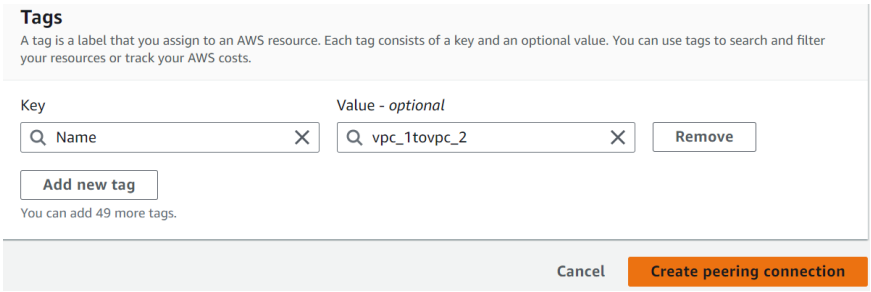
Step II : Click on Peering Connections and then click on create Peering Connections.



Step III : Give the name,then Select the requester id ,another region as our VPC in paris then Copy the VPC ID of paris and Paste it.

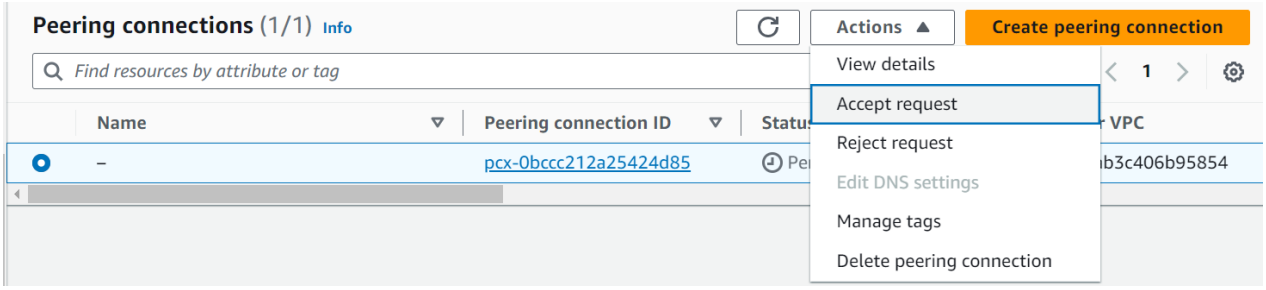


Step IV : Then, Click on create Peering Connections.

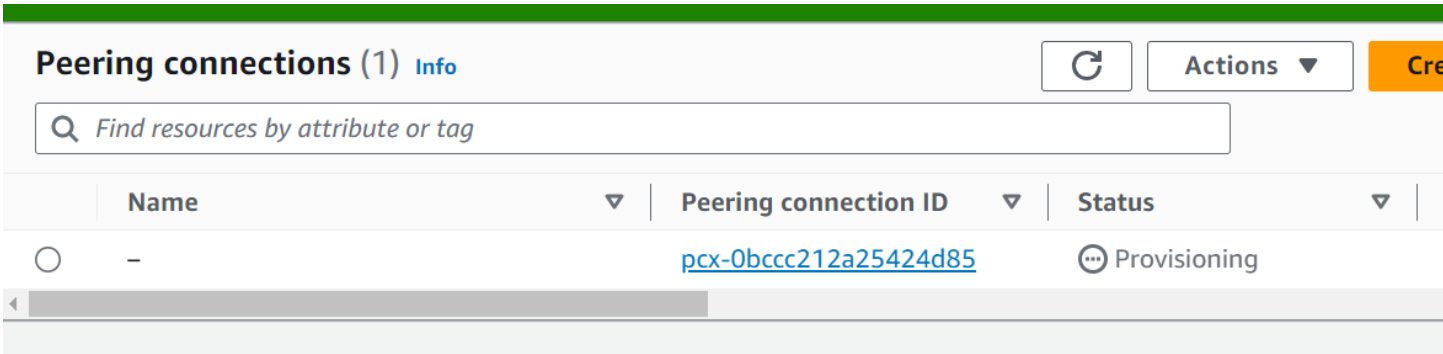


2)ACCEPT PEERING CONNECTION

Step I : Go to Paris region in Peering Connections, select the connection and click on actions then click on accept request.

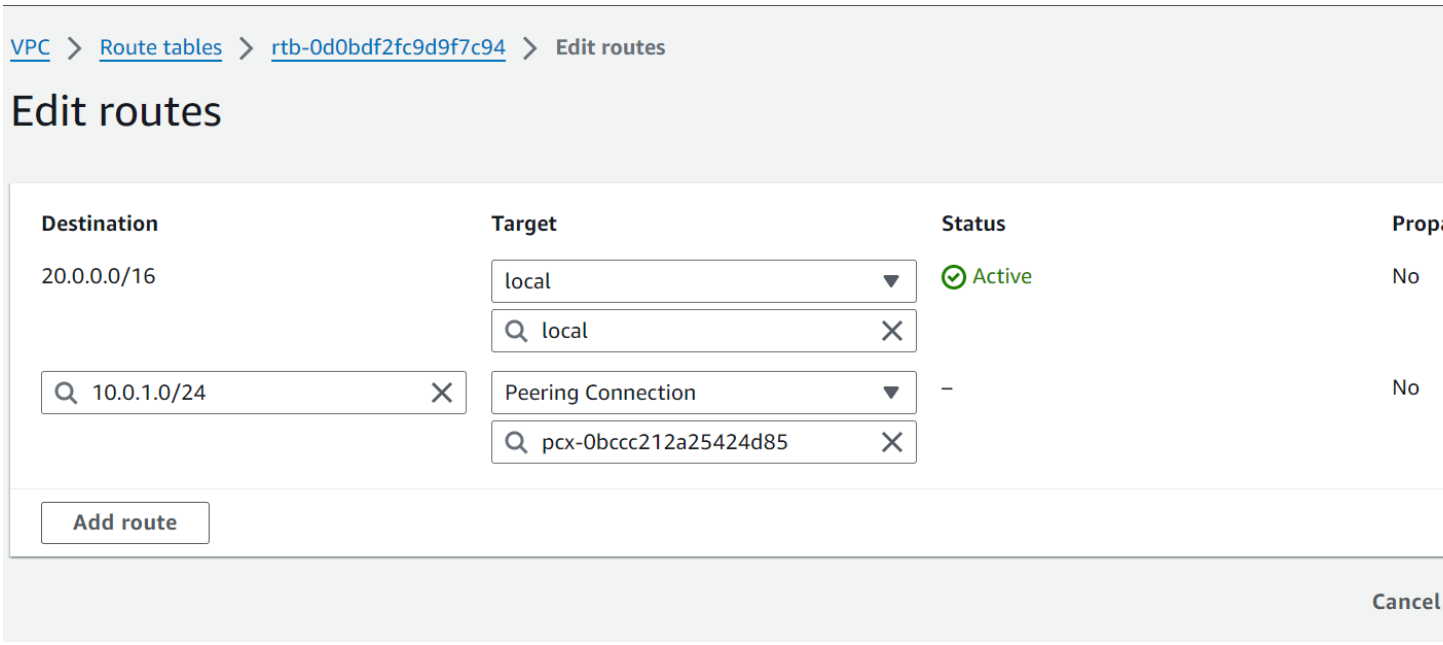


Step II : request accepted ,status is Provisioning.

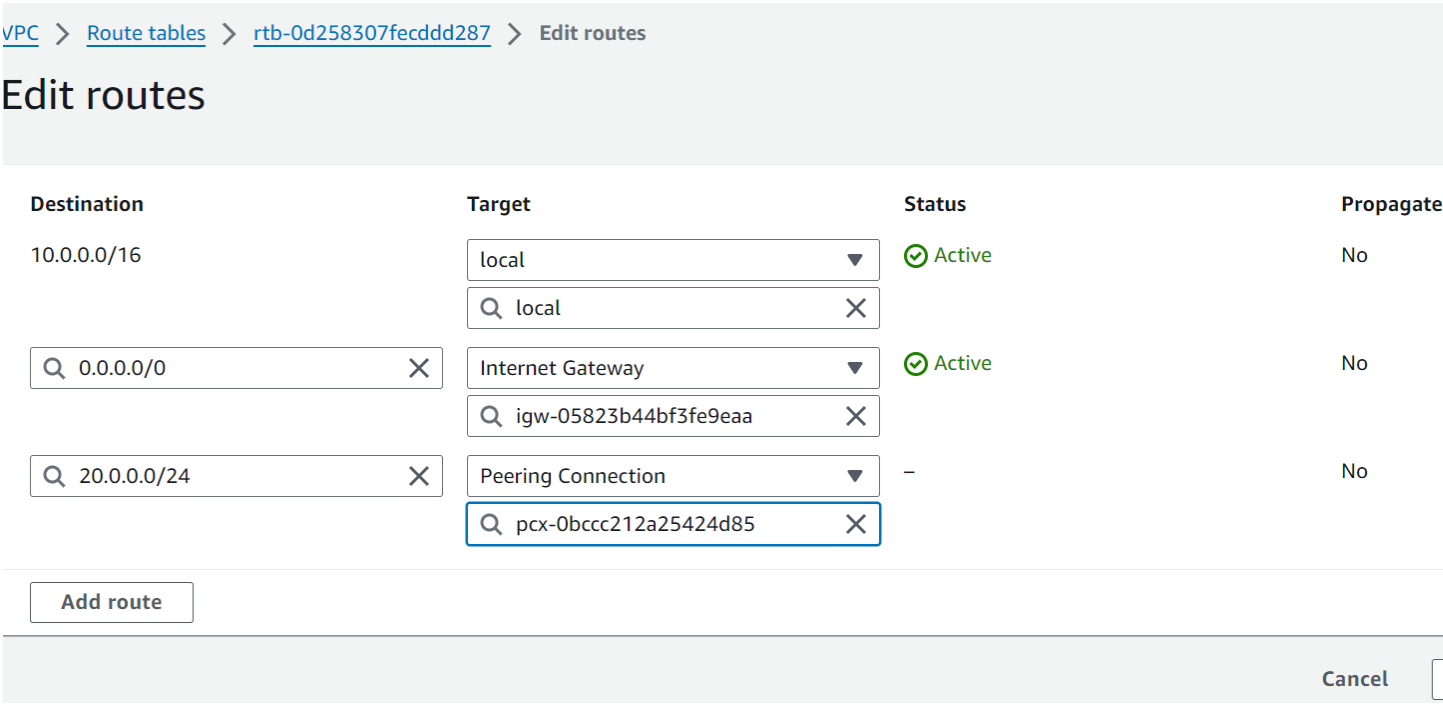


3)UPDATE ROUTE TABLES FOR PEERING CONNECTION

Step I : In Paris ,Go to the Subnet click on subnet ID ,copy the CIDR and Go back to Singapore region and click on route tables.

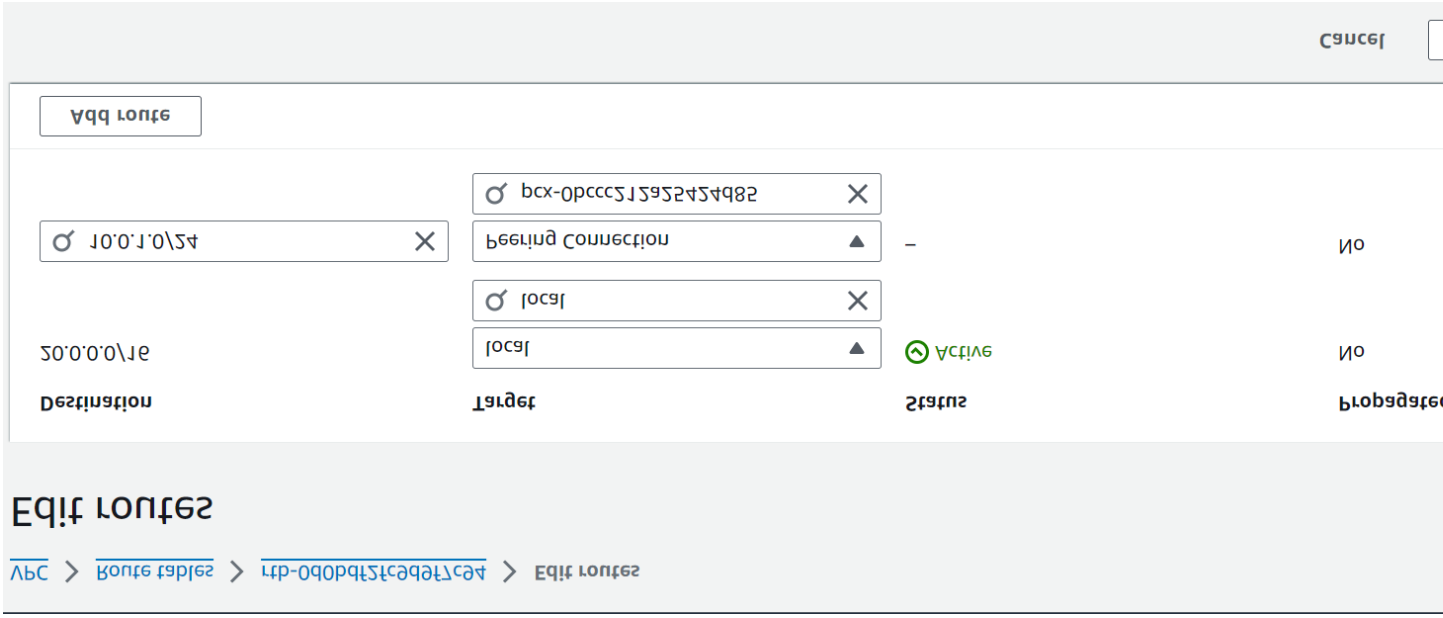


Step II : click on edit route the add route paste this CIDR in destination and choose the peering connections and the save Changes.



Step III : Now , go to the subnet of Singapore region of private Subnet.

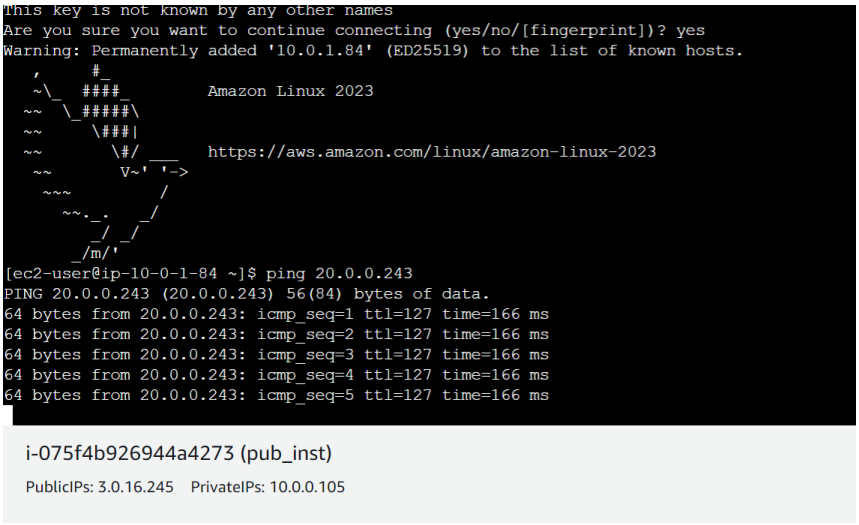
Step IV : Copy the CIDR and go to paris region in route table, click on edit and the add rule and paste CIDR and select the peering connections and then save changes.



4)CHECK CONNECTION

Step I : now copy the private IP of Private Instance and ping it on connected instance.

Step II : It is Pinged Successfully, It means Peering Connection is done.



Step III : for remote access of these instance.

Step IV: Copy the private key of private instances and paste it in vim key.pem and give the rw permission.

Step V: to give remote access of private instance give command ssh -i “keyname” ec2-user@privateIP.

Step VI : here ,we can remotely access the private IP.